

Internal Audit, Risk, Business & Technology Consulting

Blueprint for a Quantitative Cyber Risk Management Baseline

September 28, 2021

INNOVATE. TRANSFORM. SUCCEED.

Adapt to the new business reality.

protiviti[®]
Face the Future with Confidence



INTRODUCTIONS



Grace Gair,
CISSP,
CRISC, Open
FAIR
Foundations

- Senior Manager in Protiviti's Security & Privacy practice in Protiviti's NYC office.
- 9 years' experience working with both private and public sector organizations to assess and mature their Security and Risk functions. Grace specializes in Cyber Risk Quantification using the FAIR methodology and has worked with a variety of clients to analyze cyber risks and implement ongoing risk quantification programs.

- Senior Consultant in Protiviti's Security & Privacy practice in Protiviti's Chicago office.
- Jack has been involved in a variety of projects helping companies across the financial services, information management, and consumer products sectors make data-driven cybersecurity decisions using FAIR.

Jack Nelson,
Open FAIR
Foundations,
AWS
Certified
Solutions
Architect



AGENDA

What is a “baseline”?

- Risk management stack
- Definition of a baseline

4

What are the benefits of creating a baseline?

- Big-picture view
- Track over time
- Measure against appetite

14

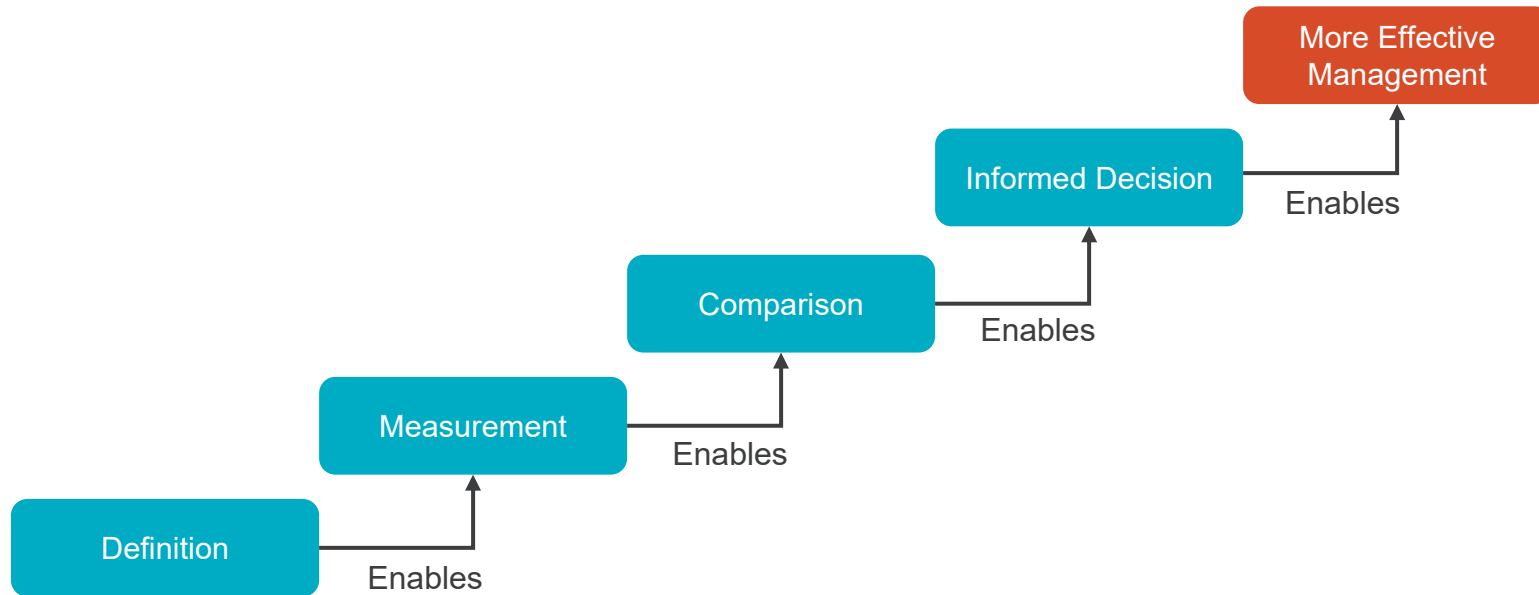
How do we build a baseline?

- The baseline cycle
- Maintenance considerations

22

What is a “Baseline”?

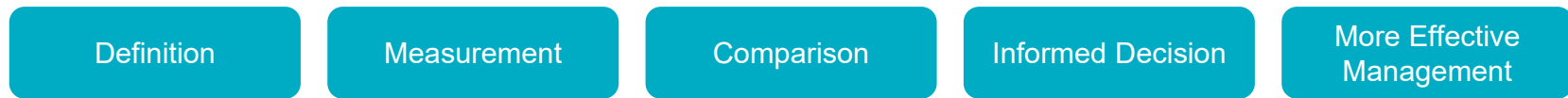
THE RISK MANAGEMENT STACK¹



¹Freund, Jack, and Jack Jones. *Measuring and Managing Information Risk : A Fair Approach*. Page 279. Elsevier, Cop, 2015.

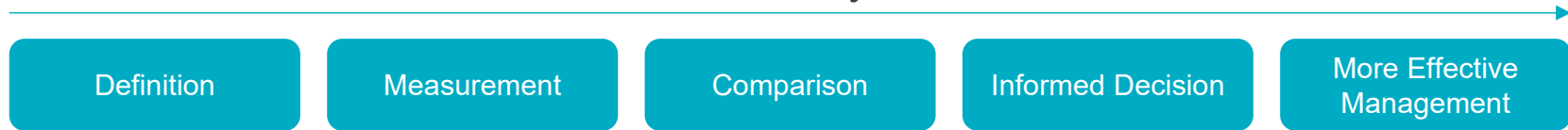
THE RISK MANAGEMENT JOURNEY

Maturity



THE RISK MANAGEMENT JOURNEY

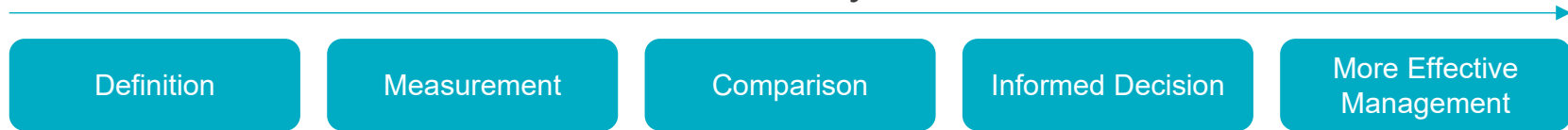
Maturity



- Establish Consistent Risk Terminology

THE RISK MANAGEMENT JOURNEY

Maturity



- Establish Consistent Risk Terminology
- Develop and Quantify Scenarios

THE RISK MANAGEMENT JOURNEY

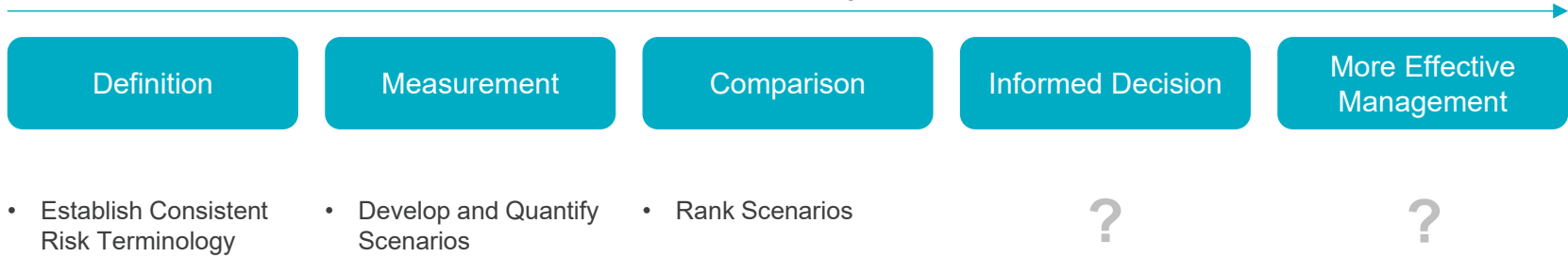
Maturity



- Establish Consistent Risk Terminology
- Develop and Quantify Scenarios
- Rank Scenarios

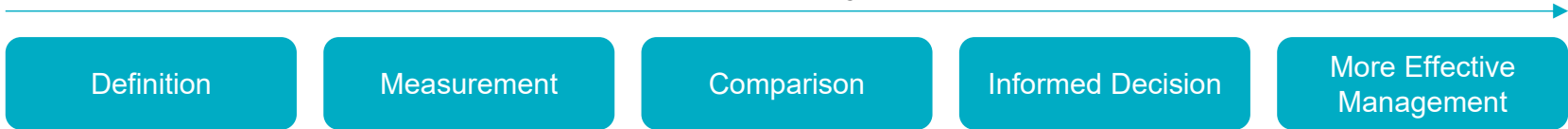
THE RISK MANAGEMENT JOURNEY

Maturity



THE RISK MANAGEMENT JOURNEY

Maturity



- Establish Consistent Risk Terminology

- Develop and Quantify Scenarios

- Rank Scenarios

?

?



Scenario 1: <\$500K



Scenario 2: <\$200K



Scenario 3: <\$10K

What's important?

What's in your fridge?



What's in your fridge?



THE RISK MANAGEMENT JOURNEY

Omelette



Created by Chrock(Green) Par from Noun Project

© 2021 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.

protiviti®

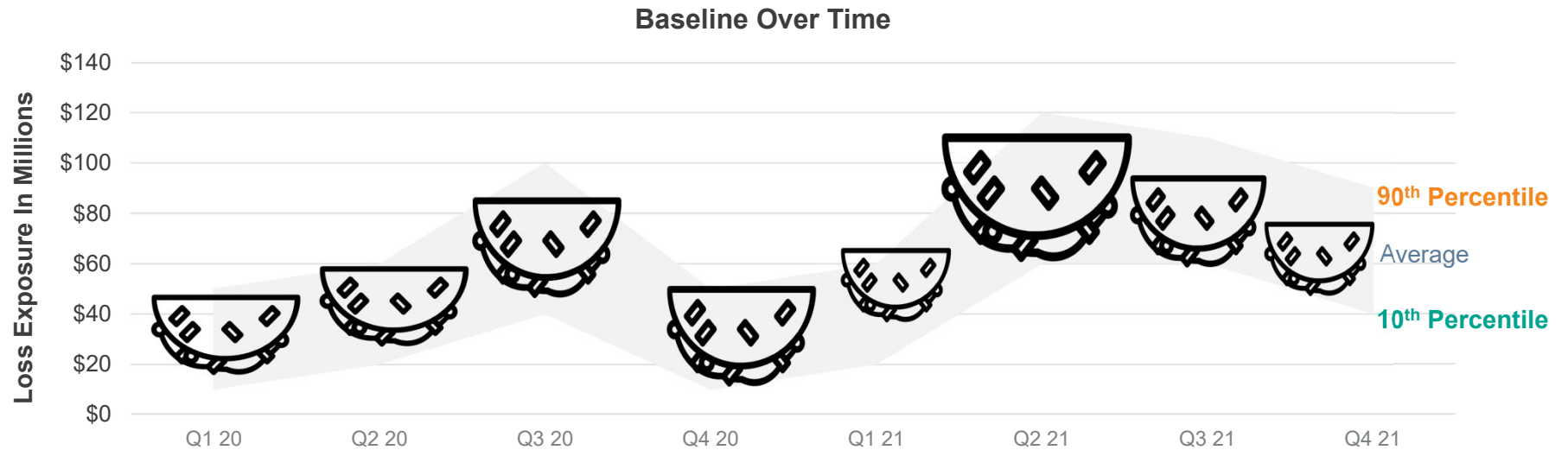
Technology Consulting

RISK BASELINE

A risk baseline is a **methodically defined and maintained, aggregate** view of loss exposure across a given domain.

RISK BASELINE

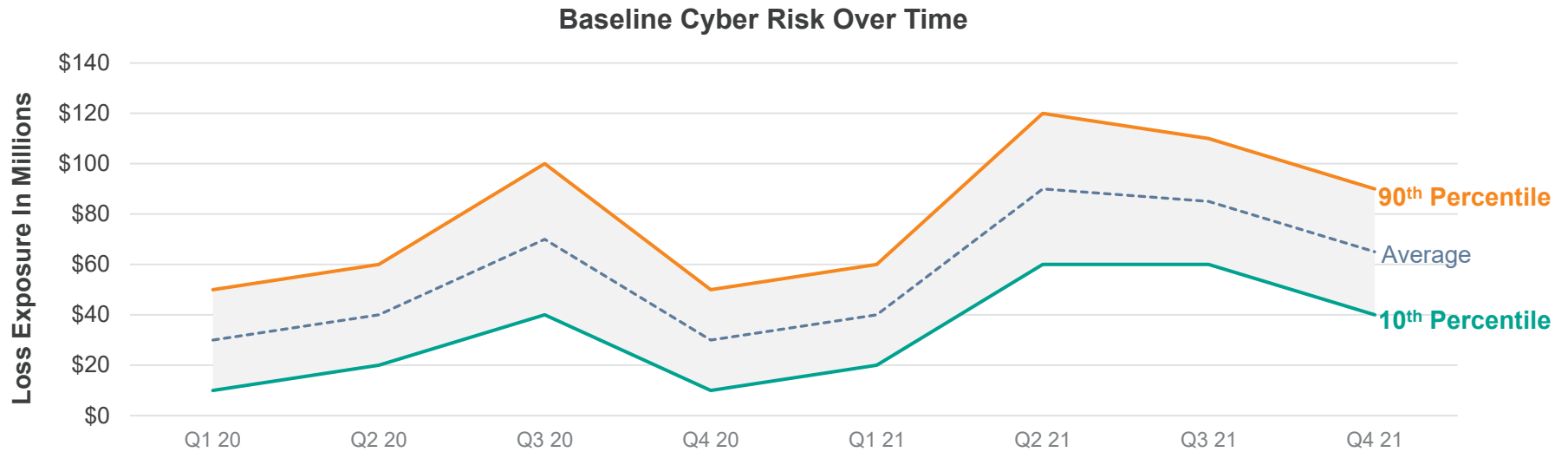
A risk baseline is a **methodically defined and maintained, aggregate** view of loss exposure across a given domain.



What are the benefits?

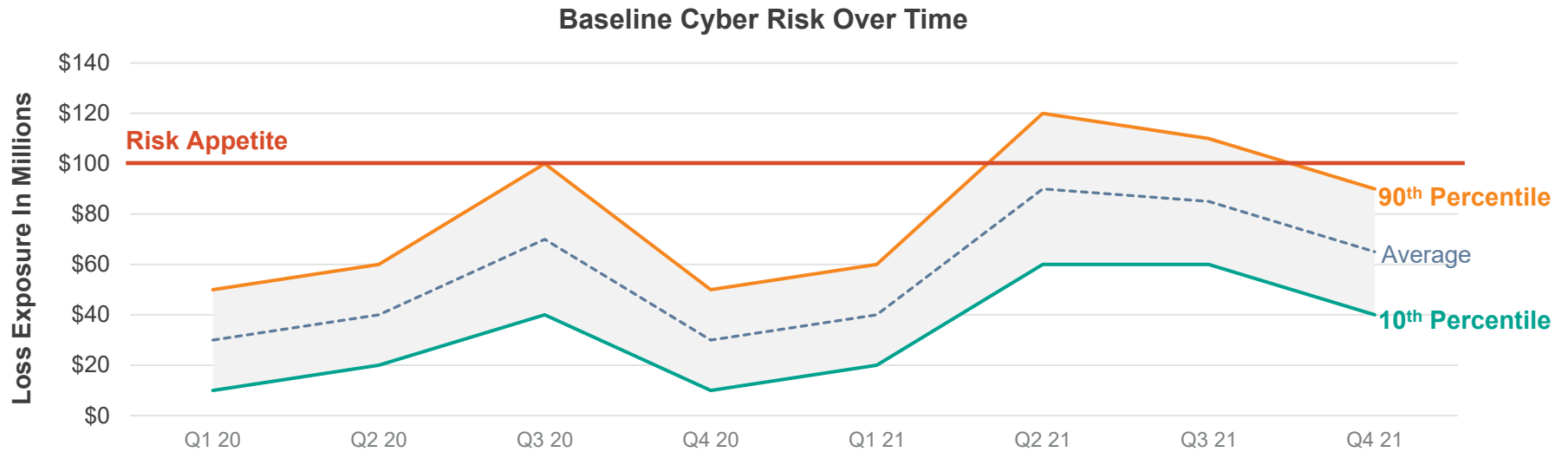
RISK BASELINE

- Baselines allow for comparison over time



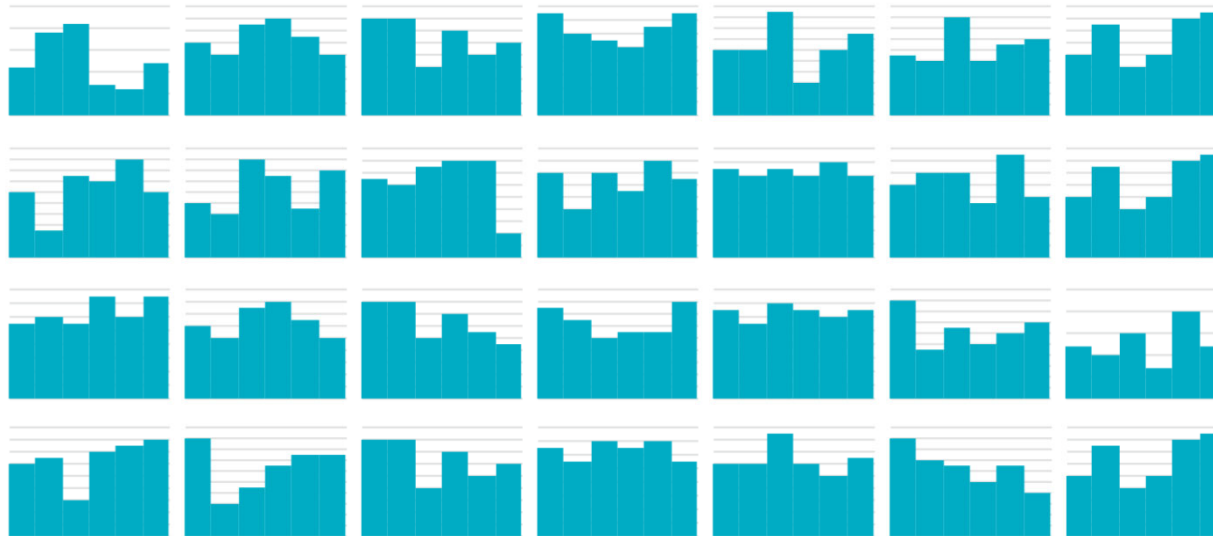
RISK BASELINE

- Baselines allow for meaningful tracking against risk appetite



RISK BASELINE

- Baselines provide a wider and **more defined** view of the risk landscape



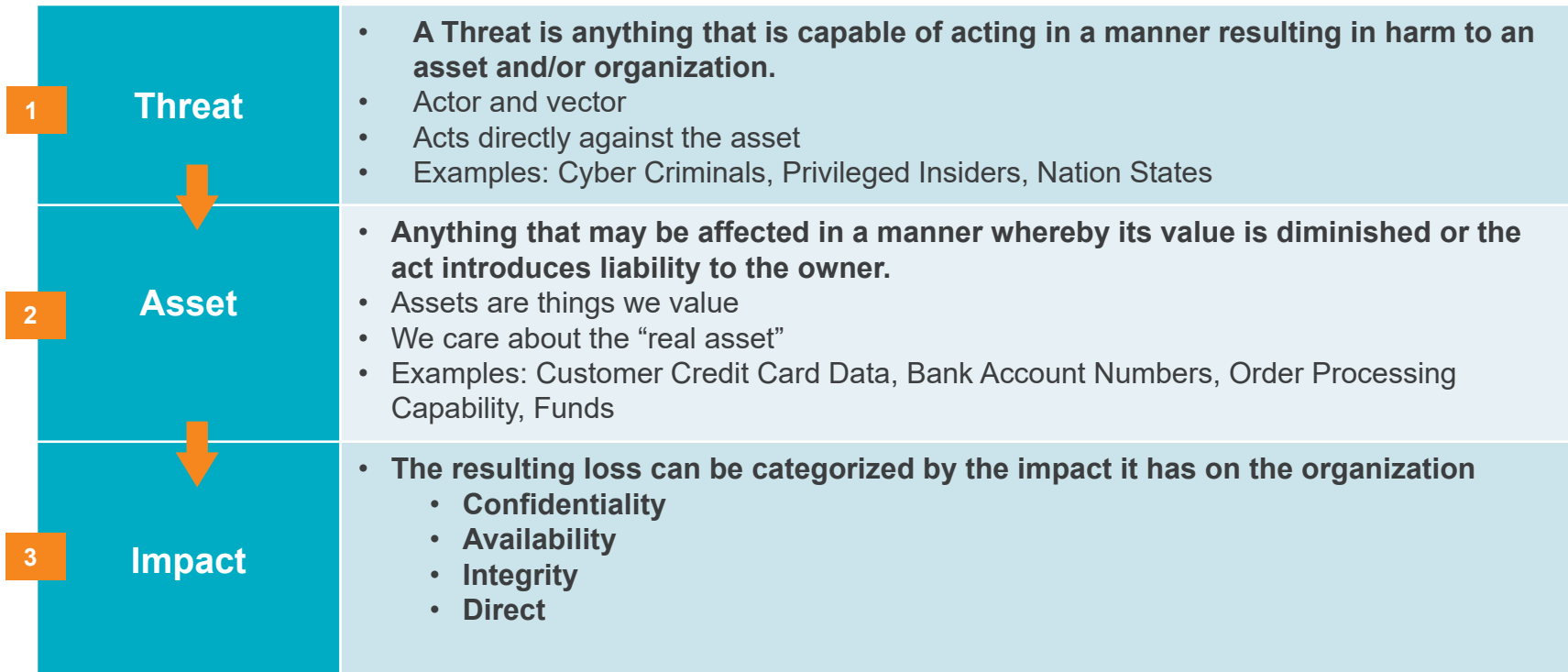
RISK BASELINE

- Baselines provide a wider and **more defined** view of the risk landscape



How do we build one?

FAIR SCENARIO RECAP



Slide 23

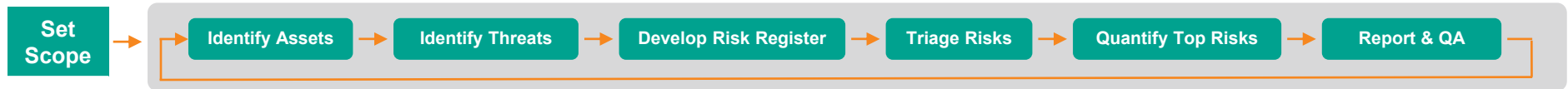
GG(1)

Add numbers

Gair, Grace (10170), 9/27/2021

BUILDING A RISK BASELINE

Risk Baseline Process



BUILDING A RISK BASELINE

Risk Baseline Process



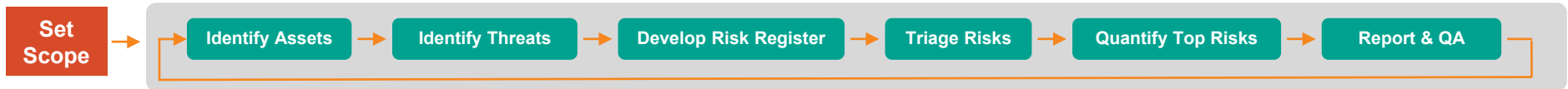
Example Process Outputs

2

Notes for Practitioners

BUILDING A RISK BASELINE

Risk Baseline Process



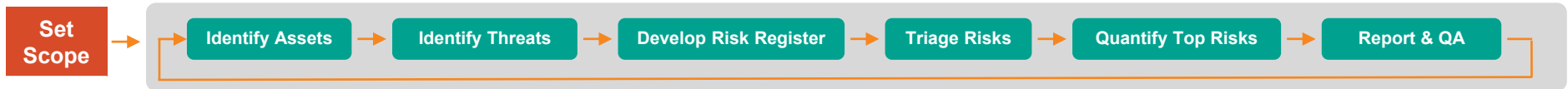
Example Process Outputs

Notes for Practitioners

- Scoping in this case refers to the scope for the baseline, rather than for a specific scenario
- Scope is usually driven by:
 - The organization's need for visibility into risk areas
 - The organization's risk categorization scheme
- Scope should be explicit as to what is and is not included

BUILDING A RISK BASELINE

Risk Baseline Process



Example Process Outputs

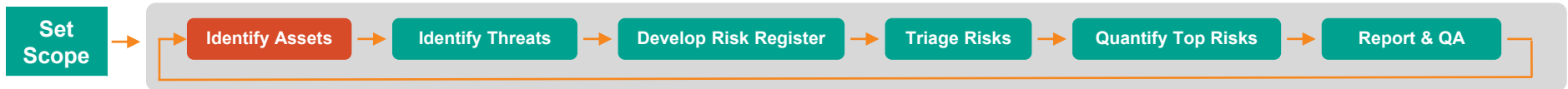
| Scope |
|------------|
| Cyber Risk |
| Cyber Risk |
| Cyber Risk |

Notes for Practitioners

- Scoping in this case refers to the scope for the baseline, rather than for a specific scenario
- Scope is usually driven by:
 - The organization's need for visibility into risk areas
 - The organization's risk categorization scheme
- Document, document, document!

BUILDING A RISK BASELINE

Risk Baseline Process



Example Process Outputs

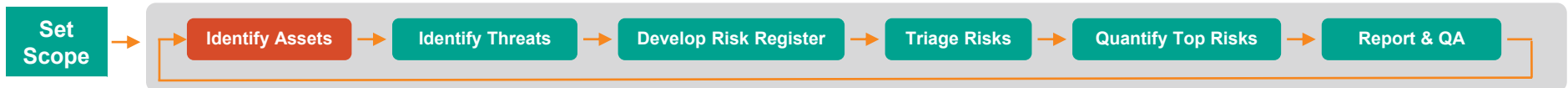
| Scope |
|------------|
| Cyber Risk |
| Cyber Risk |
| Cyber Risk |

Notes for Practitioners

- Asset discovery is recommended as the starting point for greenfield scenario development, as assets help lay groundwork for the rest of the baseline
- Asset breadth is an important factor in cases where scenarios are ultimately going to be included in a baseline; assets should generally be similar in this respect

BUILDING A RISK BASELINE

Risk Baseline Process

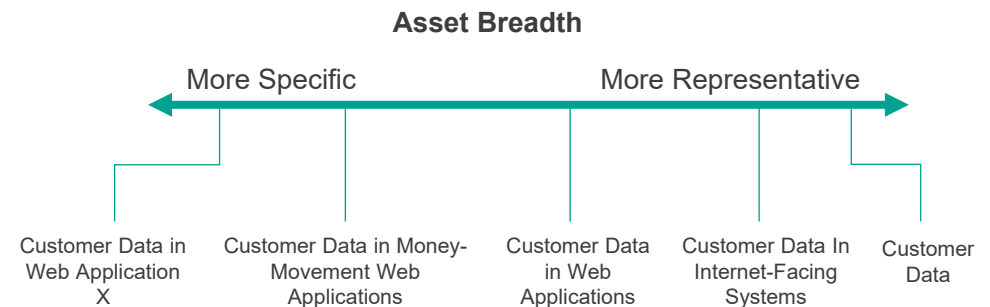


Example Process Outputs

| Scope |
|------------|
| Cyber Risk |
| Cyber Risk |
| Cyber Risk |

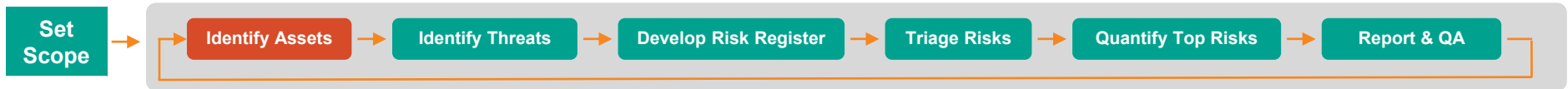
Notes for Practitioners

- Asset discovery is recommended as the starting point for greenfield scenario development, as assets help lay groundwork for the rest of the baseline
- Asset breadth is an important factor in cases where scenarios are ultimately going to be included in a baseline; assets should generally be similar in this respect



BUILDING A RISK BASELINE

Risk Baseline Process

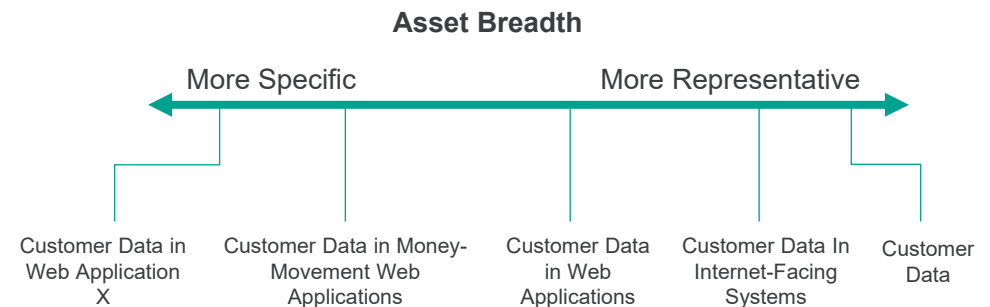


Example Process Outputs

| Scope | Asset |
|------------|----------------------------|
| Cyber Risk | Customer Data in Web App X |
| Cyber Risk | Analytics Platform Z |
| Cyber Risk | Analytics Platform Z |

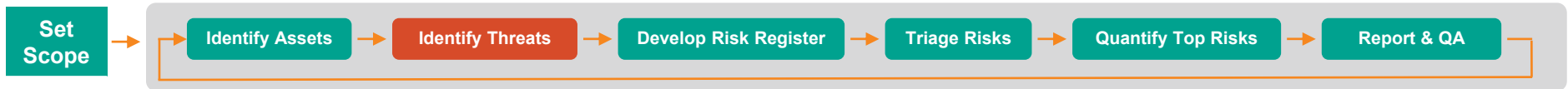
Notes for Practitioners

- Asset discovery is recommended as the starting point for greenfield scenario development, as assets help lay groundwork for the rest of the baseline
- Asset breadth is an important factor in cases where scenarios are ultimately going to be included in a baseline; assets should generally be similar in this respect



BUILDING A RISK BASELINE

Risk Baseline Process



Example Process Outputs

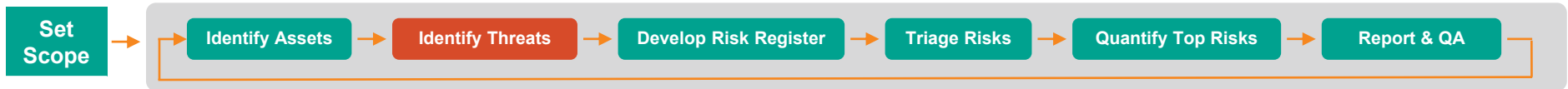
| Scope | Asset |
|------------|----------------------------|
| Cyber Risk | Customer Data in Web App X |
| Cyber Risk | Analytics Platform Z |
| Cyber Risk | Analytics Platform Z |

Notes for Practitioners

- Threat Identification should leverage information learned during asset identification
- Enterprise and industry resources should be leveraged wherever possible

BUILDING A RISK BASELINE

Risk Baseline Process



Example Process Outputs

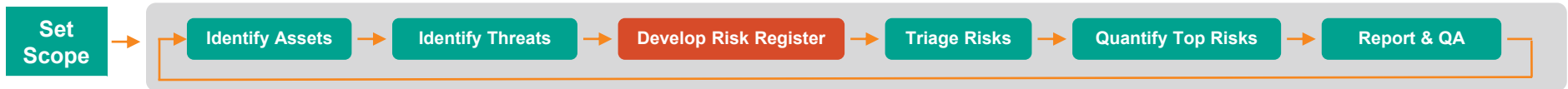
| Scope | Asset | Threat |
|------------|----------------------------|--------------------------------|
| Cyber Risk | Customer Data in Web App X | External Actor via Web Exploit |
| Cyber Risk | Analytics Platform Z | Privileged Insider via Theft |
| Cyber Risk | Analytics Platform Z | External Actor via Web Exploit |

Notes for Practitioners

- Threat Identification should leverage information learned during asset identification
- Enterprise and industry resources should be leveraged wherever possible

BUILDING A RISK BASELINE

Risk Baseline Process



Example Process Outputs

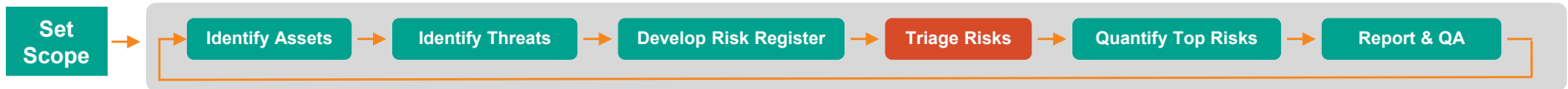
| Scope | Asset | Threat | Risk |
|------------|----------------------------|--------------------------------|---|
| Cyber Risk | Customer Data in Web App X | External Actor via Web Exploit | External Actor breaches Web App X. |
| Cyber Risk | Analytics Platform Z | Privileged Insider via Theft | Insider steals records from Analytics Platform Z. |
| Cyber Risk | Analytics Platform Z | External Actor via Web Exploit | External Actor breaches Analytics Platform Z. |

Notes for Practitioners

- When assets and threats are combined with impacts to create FAIR-compliant scenarios, the result is an inventory of risks
- Analysts should leverage their own intuition to understand which threat-asset pairings are likely and lean toward a more-inclusive approach
- When the inventory is too large to quantify, triage is used to reduce the number of baseline-eligible scenarios

BUILDING A RISK BASELINE

Risk Baseline Process



Example Process Outputs

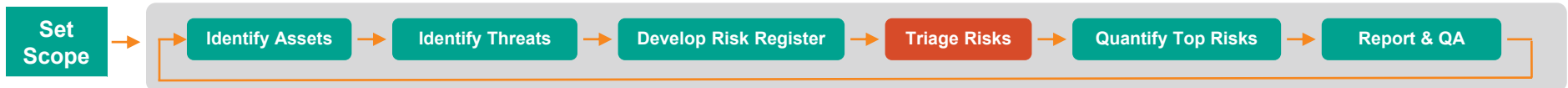
| Scope | Asset | Threat | Risk |
|------------|----------------------------|--------------------------------|---|
| Cyber Risk | Customer Data in Web App X | External Actor via Web Exploit | External Actor breaches Web App X. |
| Cyber Risk | Analytics Platform Z | Privileged Insider via Theft | Insider steals records from Analytics Platform Z. |
| Cyber Risk | Analytics Platform Z | External Actor via Web Exploit | External Actor breaches Analytics Platform Z. |

Notes for Practitioners

- Triage uses broader ranges and a heavier dependence on calibrated estimation to identify which risks are likely to account for the largest share of the population

BUILDING A RISK BASELINE

Risk Baseline Process



Example Process Outputs

| Scope | Asset | Threat | Risk |
|------------|----------------------------|--------------------------------|---|
| Cyber Risk | Customer Data in Web App X | External Actor via Web Exploit | External Actor breaches Web App X. |
| Cyber Risk | Analytics Platform Z | Privileged Insider via Theft | Insider steals records from Analytics Platform Z. |
| Cyber Risk | Analytics Platform Z | External Actor via Web Exploit | External Actor breaches Analytics Platform Z. |

Notes for Practitioners

- Triage uses broader ranges and a heavier dependence on calibrated estimation to identify which risks are likely to account for the largest share of the population
- By doing triage quantitatively, rather than qualitatively, it is possible to calculate the expected coverage of the baseline



Scenario 1: <\$500K



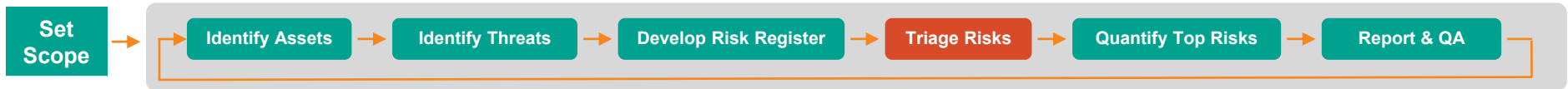
Scenario 2: <\$200K



Scenario 3: <\$10K

BUILDING A RISK BASELINE

Risk Baseline Process



Example Process Outputs

| Scope | Asset | Threat | Risk |
|------------|----------------------------|--------------------------------|---|
| Cyber Risk | Customer Data in Web App X | External Actor via Web Exploit | External Actor breaches Web App X. |
| Cyber Risk | Analytics Platform Z | Privileged Insider via Theft | Insider steals records from Analytics Platform Z. |
| Cyber Risk | Analytics Platform Z | External Actor via Web Exploit | External Actor breaches Analytics Platform Z. |

Notes for Practitioners

- Triage uses broader ranges and a heavier dependence on calibrated estimation to identify which risks are likely to account for the largest share of the population
- By doing triage quantitatively, rather than qualitatively, it is possible to calculate the expected coverage of the baseline



Scenario 1: <\$500K



Scenario 2: <\$200K

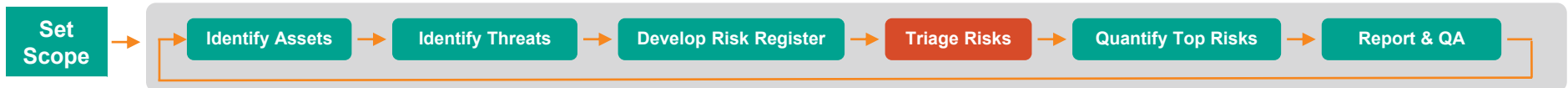


Scenario 3: <\$10K

**98%
Coverage**

BUILDING A RISK BASELINE

Risk Baseline Process



Example Process Outputs

| Scope | Asset | Threat | Risk | Loss Exposure |
|------------|----------------------------|--------------------------------|---|---------------|
| Cyber Risk | Customer Data in Web App X | External Actor via Web Exploit | External Actor breaches Web App X. | <\$10M |
| Cyber Risk | Analytics Platform Z | Privileged Insider via Theft | Insider steals records from Analytics Platform Z. | <\$500K |
| Cyber Risk | Analytics Platform Z | External Actor via Web Exploit | External Actor breaches Analytics Platform Z. | <\$15M |

Notes for Practitioners

- Triage uses broader ranges and a heavier dependence on calibrated estimation to identify which risks are likely to account for the largest share of the population
- By doing triage quantitatively, rather than qualitatively, it is possible to calculate the expected coverage of the baseline



Scenario 1: <\$500K



Scenario 2: <\$200K

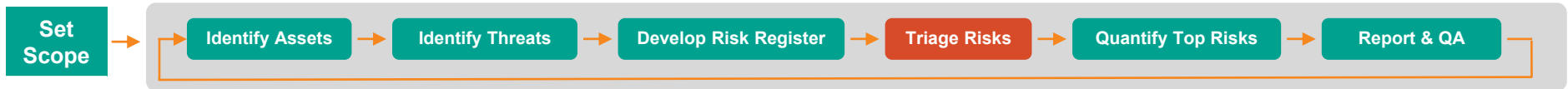


Scenario 3: <\$10K

**98%
Coverage**

BUILDING A RISK BASELINE

Risk Baseline Process



Example Process Outputs

| Scope | Asset | Threat | Risk | Loss Exposure |
|------------|----------------------------|--------------------------------|---|---------------|
| Cyber Risk | Customer Data in Web App X | External Actor via Web Exploit | External Actor breaches Web App X. | <\$10M |
| Cyber Risk | Analytics Platform Z | Privileged Insider via Theft | Insider steals records from Analytics Platform Z. | <\$500K |
| Cyber Risk | Analytics Platform Z | External Actor via Web Exploit | External Actor breaches Analytics Platform Z. | <\$15M |

Notes for Practitioners

- Triage uses broader ranges and a heavier dependence on calibrated estimation to identify which risks are likely to account for the largest share of the population
- By doing triage quantitatively, rather than qualitatively, it is possible to calculate the expected coverage of the baseline



Scenario 1: <\$500K



Scenario 2: <\$200K

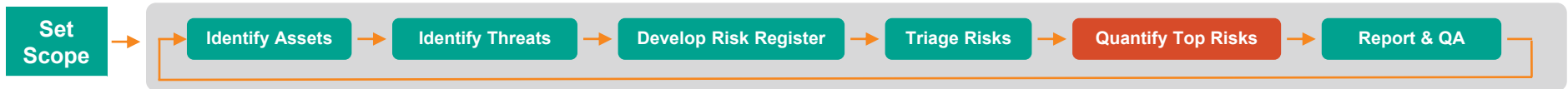


Scenario 3: <\$10K

98% Coverage

BUILDING A RISK BASELINE

Risk Baseline Process



Example Process Outputs

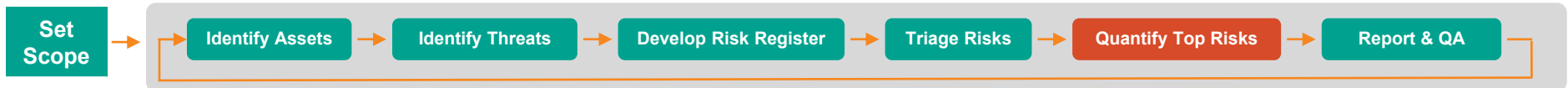
| Scope | Asset | Threat | Risk | Loss Exposure |
|------------|----------------------------|--------------------------------|---|---------------|
| Cyber Risk | Customer Data in Web App X | External Actor via Web Exploit | External Actor breaches Web App X. | <\$10M |
| Cyber Risk | Analytics Platform Z | Privileged Insider via Theft | Insider steals records from Analytics Platform Z. | <\$500K |
| Cyber Risk | Analytics Platform Z | External Actor via Web Exploit | External Actor breaches Analytics Platform Z. | <\$15M |

Notes for Practitioners

- Risks selected for full-scope analysis are analyzed using FAIR best practices
- Scenarios can be removed or added to the baseline after full quantification based on outcome

BUILDING A RISK BASELINE

Risk Baseline Process



Example Process Outputs

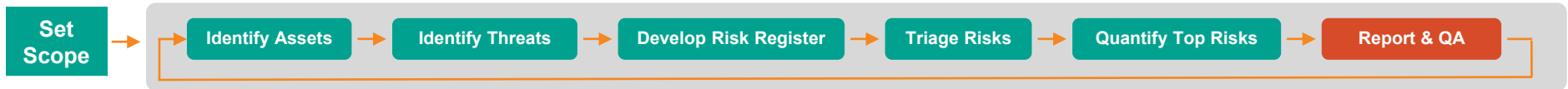
| Scope | Asset | Threat | Risk | Loss Exposure |
|------------|----------------------------|--------------------------------|---|---------------|
| Cyber Risk | Customer Data in Web App X | External Actor via Web Exploit | External Actor breaches Web App X. | \$6.75M |
| Cyber Risk | Analytics Platform Z | Privileged Insider via Theft | Insider steals records from Analytics Platform Z. | <\$500K |
| Cyber Risk | Analytics Platform Z | External Actor via Web Exploit | External Actor breaches Analytics Platform Z. | \$10.12M |

Notes for Practitioners

- Risks selected for full-scope analysis are analyzed using FAIR best practices
- Scenarios can be removed or added to the baseline after full quantification based on outcome

BUILDING A RISK BASELINE

Risk Baseline Process



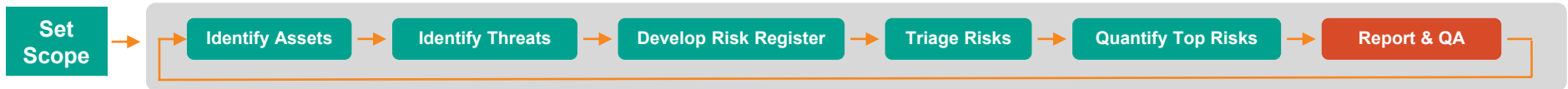
Example Process Outputs

| Scope | Asset | Threat | Risk | Loss Exposure |
|------------|----------------------------|--------------------------------|---|---------------|
| Cyber Risk | Customer Data in Web App X | External Actor via Web Exploit | External Actor breaches Web App X. | \$6.75M |
| Cyber Risk | Analytics Platform Z | Privileged Insider via Theft | Insider steals records from Analytics Platform Z. | <\$500K |
| Cyber Risk | Analytics Platform Z | External Actor via Web Exploit | External Actor breaches Analytics Platform Z. | \$10.12M |

Q1 Risk Baseline: \$16M

BUILDING A RISK BASELINE

Risk Baseline Process



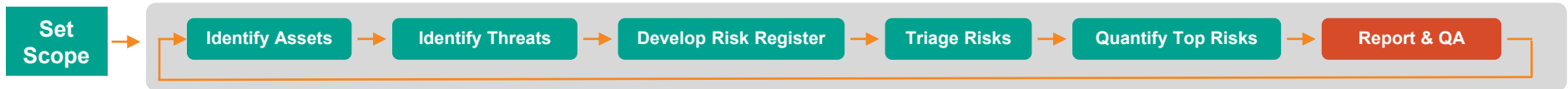
Example Process Outputs

| Scope | Asset | Threat | Risk | Loss Exposure |
|------------|----------------------------|--------------------------------|---|---------------|
| Cyber Risk | Customer Data in Web App X | External Actor via Web Exploit | External Actor breaches Web App X. | \$7.75M |
| Cyber Risk | Analytics Platform Z | Privileged Insider via Theft | Insider steals records from Analytics Platform Z. | <\$500K |
| Cyber Risk | Analytics Platform Z | External Actor via Web Exploit | External Actor breaches Analytics Platform Z. | \$11.12M |

Q1 Risk Baseline: \$8.5M Q2 Risk Baseline: \$19M

BUILDING A RISK BASELINE

Risk Baseline Process



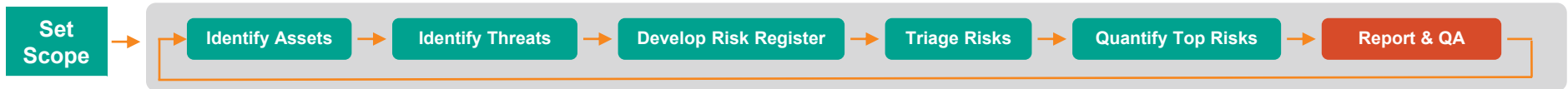
Example Process Outputs

| Scope | Asset | Threat | Risk | Loss Exposure |
|------------|----------------------------|--------------------------------|---|---------------|
| Cyber Risk | Customer Data in Web App X | External Actor via Web Exploit | External Actor breaches Web App X. | \$10.75M |
| Cyber Risk | Analytics Platform Z | Privileged Insider via Theft | Insider steals records from Analytics Platform Z. | <\$500K |
| Cyber Risk | Analytics Platform Z | External Actor via Web Exploit | External Actor breaches Analytics Platform Z. | \$11.12M |

Q1 Risk Baseline: \$8.5M Q2 Risk Baseline: \$19M Q2 Risk Baseline: \$22M

BUILDING A RISK BASELINE

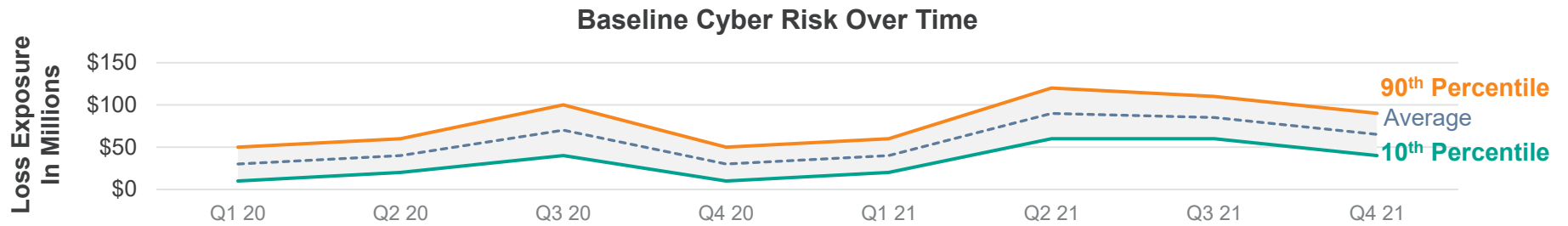
Risk Baseline Process



Example Process Outputs

| Scope | Asset | Threat | Risk | Loss Exposure |
|------------|----------------------------|--------------------------------|---|---------------|
| Cyber Risk | Customer Data in Web App X | External Actor via Web Exploit | External Actor breaches Web App X. | \$10.75M |
| Cyber Risk | Analytics Platform Z | Privileged Insider via Theft | Insider steals records from Analytics Platform Z. | <\$500K |
| Cyber Risk | Analytics Platform Z | External Actor via Web Exploit | External Actor breaches Analytics Platform Z. | \$11.12M |

Q1 Risk Baseline: \$8.5M Q2 Risk Baseline: \$19M Q2 Risk Baseline: \$22M



NOTES ON GOVERNANCE

- Process governance is critical to ongoing baseline reputability
 - Update procedures should be documented and conducted on a defined cadence
 - When do we begin the cycle again?
 - What level of review is required for scope changes?
 - Qualifications should be established for the introduction or removal of scenarios from the baseline

CLOSING THOUGHTS

- Risk baselining is a powerful tool that enables organizations to focus on what matters, understand their larger risk landscape, and see clearly how risk is trending over time
- Baselines should be held to standards to ensure reputability and consistency
- Ongoing process, it's okay to refine things!

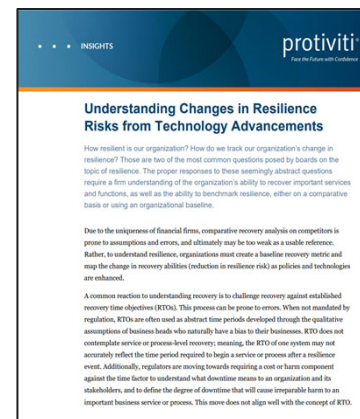
Q&A

For the latest Protiviti-developed materials on Cyber Risk Quantification, visit:

www.protiviti.com/fair

Protiviti Subject Matter Experts:

- **Grace Gair** – grace.gair@protiviti.com
- **Jack Nelson** – jack.nelson@protiviti.com



INSIGHTS protiviti
For the Future with Confidence

Understanding Changes in Resilience Risks from Technology Advancements

How resilient is our organization? How do we track our organization's change in resilience? Those are two of the most common questions posed by boards on the topic of resilience. The proper responses to these seemingly abstract questions require a firm understanding of the organization's ability to recover important services and functions, as well as the ability to benchmark resilience, either on a comparative basis or using an organizational baseline.

Due to the uniqueness of financial firms, comparative recovery analysis on competitors is prone to assumptions and errors, and ultimately may be too weak as a usable reference. Rather, to understand resilience, organizations must create a baseline recovery metric and map the change in recovery abilities (reduction in resilience risk) as policies and technologies are enhanced.

A common mistake to understanding recovery is to challenge recovery against established recovery time objectives (RTOs). This process can be prone to errors. When not mandated by regulation, RTOs are often used as abstract time periods developed through the qualitative assumptions of business heads who naturally have a bias to their businesses. RTO does not contemplate service or process-level recovery; essentially, the RTO of one system may not accurately reflect the time period required to begin a service or process after a resilience event. Additionally, regulators are moving towards requiring a cost or harm component against the time factor to understand what downtime means to an organization and its stakeholders, and to define the degree of downtime that will cause irreparable harm to an important business service or process. This move does not align well with the concept of RTO.

Insight: Understanding Changes in Resilience Risk from Technology Advancements



protiviti
For the Future with Confidence

Measuring Cyber Risk Quantitatively – Eliminating the Guesswork

The Benefits of Leveraging FAIR

Internal Audit, Risk, Business & Technology Consulting

Case Study: Measuring Cyber Risk Quantitatively – Eliminating the Guesswork

Face the Future with Confidence

© 2021 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. PRO-0619
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.

protiviti®